

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

PATRICK YOCKEY, et al.,  
Plaintiffs,  
v.  
SALESFORCE, INC.,  
Defendant.

Case No. 22-cv-09067-JST

**ORDER GRANTING IN PART AND  
DENYING IN PART MOTION TO  
DISMISS**

Re: ECF No. 23

Before the Court is Defendant Salesforce, Inc.’s motion to dismiss. ECF No. 23. The Court will grant the motion in part and deny it in part.

**I. BACKGROUND**

Salesforce is a software-as-a-service provider that offers a service called Chat. ECF No. 22 ¶¶ 6, 11. Chat is an application programming interface (“API”), *id.* ¶ 12, which is “a tool that ‘allow[s] programmers to use . . . prewritten code to build certain functions into their own programs, rather than write their own code to perform those functions from scratch,” *Google LLC v. Oracle Am., Inc.*, 141 S. Ct. 1183, 1191 (2021) (quoting *Oracle Am., Inc. v. Google, Inc.*, 750 F.3d 1339, 1349 (2014)). “An API divides and organizes the world of computing tasks in a particular way.” *Id.* at 1192. *Id.* Chat operates from Salesforce’s web servers, but its functionality can be implemented on the website of a company that contracts with Salesforce to use the service, thereby allowing that company’s customers to interact with the company directly on the website. ECF No. 22 ¶ 12–13. When a customer sends a chat message to a company’s customer service agent, “it is first routed through a Salesforce server.” *Id.* ¶ 13. Transcripts of communications over Chat are automatically created in real time and subsequently transmitted to the contracting company. *Id.* ¶ 15. Chat includes a “Sneak Peek” feature, which enables an agent

1 to view the contents of a customer’s message while the customer types the message, *i.e.*, before  
2 the customer sends the message to the agent. *Id.* ¶ 22–23.

3 Rite Aid and Kaiser Permanente utilize Chat on their websites. *Id.* ¶ 13. Plaintiff Pearl  
4 Magpayo is a California resident and used the chat function on the Kaiser Permanente website to  
5 discuss her insurance and medical information with Kaiser’s customer service agents. *Id.* ¶ 4.  
6 Plaintiff Patrick Yockey is a Pennsylvania resident and used the chat function on the Rite Aid  
7 website to discuss his prescription history and customer rewards with Rite Aid’s customer service  
8 agents. *Id.* ¶ 3. Plaintiffs subsequently brought suit, alleging that Chat’s functions constitute  
9 wiretapping in violation of California and Pennsylvania law. As individuals and on behalf of a  
10 putative class, they bring claims for violations of the California Invasion of Privacy Act (“CIPA”),  
11 Cal. Penal Code §§ 631 & 632; and violation of Pennsylvania’s Wiretapping and Electronic  
12 Surveillance Control Act (“WESCA”), 18 Pa. Cons. Stat. § 5701, *et seq.* ECF No. 22 ¶¶ 48–80.

13 Salesforce moved to dismiss the complaint on April 24, 2023. ECF No. 23. The Court  
14 took the motion under submission without a hearing on July 17, 2023. ECF No. 33.

## 15 **II. JURISDICTION**

16 The Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A).

## 17 **III. LEGAL STANDARD**

18 To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a  
19 complaint must contain “a short and plain statement of the claim showing that the pleader is  
20 entitled to relief.” Fed. R. Civ. P. 8(a)(2). Dismissal “is appropriate only where the complaint  
21 lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory.”  
22 *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). “[A] complaint  
23 must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible  
24 on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*,  
25 550 U.S. 544, 570 (2007)). Factual allegations need not be detailed, but facts must be “enough to  
26 raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555.

27 “A claim has facial plausibility when the plaintiff pleads factual content that allows the  
28 court to draw the reasonable inference that the defendant is liable for the misconduct

alleged.” *Iqbal*, 556 U.S. at 678. While this standard is not “akin to a ‘probability requirement,’ . . . it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (quoting *Twombly*, 550 U.S. at 556). “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’” *Id.* (quoting *Twombly*, 550 U.S. at 557). In determining whether a plaintiff has met the plausibility requirement, a court must “accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable” to the plaintiff. *Kniesel v. ESPN*, 393 F.3d 1068, 1072 (9th Cir. 2005). A plaintiff may “plead[] facts alleged upon information and belief where the facts are peculiarly within the possession and control of the defendant or where the belief is based on factual information that makes the inference of culpability plausible.” *Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (quoting *Arista Records, LLC v. Doe 3*, 603 F.3d 110, 120 (2d Cir. 2010)).

#### IV. DISCUSSION

Salesforce argues that Plaintiffs lack standing, that Plaintiffs fail to state a claim under either statute, and that Plaintiffs otherwise consented to Salesforce’s collection of their information.

##### A. Article III Standing

“Article III of the Constitution confines the federal judicial power to the resolution of ‘Cases’ and ‘Controversies.’” *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). “For there to be a case or controversy under Article III, the plaintiff must have a ‘personal stake’ in the case—in other words, standing.” *Id.* (quoting *Raines v. Byrd*, 521 U.S. 811, 819 (1997)). “[T]o establish standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant, and (iii) that the injury would likely be redressed by judicial relief.” *Id.* at 2203. “The party invoking federal jurisdiction bears the burden of establishing these elements.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). “Where, as here, a case is at the pleading stage, the plaintiff must ‘clearly . . . allege facts demonstrating’ each element.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

Salesforce argues that Plaintiffs have not suffered a concrete injury because they have not alleged that Salesforce “shared, disclosed, or sold chat transcripts to third parties.” ECF No. 23 at 16. The Court is not persuaded. “[V]arious intangible harms can . . . be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts.” *TransUnion*, 141 S. Ct. at 2204. An “exact duplicate” is not required, and the Supreme Court has recognized that “intrusion upon seclusion” is included among those traditionally recognized harms. *Id.* at 2204; *see* Restatement (Second) of Torts § 652B cmt. b. (1977) (including “tapping . . . telephone wires” as an example of intrusion upon seclusion). In that vein, the Ninth Circuit has written that “[v]iolations of the right to privacy have long been actionable at common law,” and that “[a] right to privacy ‘encompass[es] the individual’s control of information concerning his or her person.’” *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 598 (9th Cir. 2020) (first quoting *Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019); and then quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)); *see also* Restatement (Second) of Torts § 652B cmt. a. (explaining that intrusion upon seclusion “does not depend upon any publicity given to the person whose interest is invaded or to his affairs” but rather “consists solely of an intentional interference with his interest in solicitude or seclusion”).

Statutes such as CIPA and WESCA thus “codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing.” *Id.*; *accord In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019) (“History and tradition reinforce that a concrete injury for Article III standing purposes occurs when Google, or any other third party, *tracks* a person’s internet browser activity without authorization.” (emphasis added)). Both Plaintiffs allege that they disclosed personal health information over Chat and that Salesforce collected the communications containing that information. ECF No. 22 ¶¶ 3, 4. These allegations give rise to a concrete injury because Salesforce’s collection of those communications necessarily deprived Plaintiffs of their control of their information contained therein. *See Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1138 (E.D. Cal. 2021); *see also Licea v. Cinmar, LLC*, --- F. Supp. 3d ---, No. CV 22-6454-MWF (JEM), 2023 WL 2415592, at \*3 (C.D. Cal. Mar. 7, 2023). Accordingly, the Court concludes that

Plaintiffs have standing to bring their claims.

## **B. CIPA**

### **1. Section 631**

Salesforce argues that Magpayo fails to state a Section 631 claim because Salesforce was “acting merely as an extension of . . . Kaiser’s communications” such that it was a party to those communications. ECF No. 23 at 22. Plaintiffs argue that Salesforce’s interpretation of Section 631 runs afoul of the statute’s text and corresponding caselaw. ECF No. 28 at 11.

Section 631 creates four avenues for relief:

(1) where a person “by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection ... with any telegraph or telephone wire, line, cable, or instrument”;

(2) where a person “willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit”;

(3) where a person “uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained”; and

(4) where a person “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above.”

*Javier v. Assurance IQ, LLC*, --- F. Supp. 3d ----, No. 20-cv-02860-CRB, 2023 WL 114225, at \*4 (N.D. Cal. Jan. 5, 2023) (quoting Cal. Penal Code § 631). Magpayo’s Section 631 claim arises under the second prong.

Recent Section 631 jurisprudence stems from two seminal cases: *Ribas v. Clark*, 38 Cal. 3d 355 (1985), and *Rogers v. Ulrich*, 52 Cal. App. 3d 894 (1975). In *Ribas*, Ribas and his former wife had reached a settlement agreement during divorce proceedings. 38 Cal. 3d at 358. The wife used Clark’s phone to call Ribas and asked Clark to listen to the conversation on an extension telephone. *Id.* Ribas relayed to the wife the details of a conversation with the spouse’s lawyer while Clark listened. *Id.* Ribas subsequently sued Clark for eavesdropping under Section 631. The California Supreme Court held that Clark’s conduct violated Section 631 because the statute

1 draws a distinction between “the secondhand repetition of the contents of a conversation and its  
2 simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or  
3 mechanical device.” *Id.* at 361. The Court wrote that “such secret monitoring denies the speaker  
4 an important aspect of privacy of communication—the right to control the nature and extent of the  
5 firsthand dissemination of his statements.” *Id.*

6 In *Rogers*, Ulrich used a tape recorder jack installed on his telephone to record a  
7 conversation with Rogers without Rogers’ knowledge. 52 Cal. App. 3d at 897. The Court of  
8 Appeal held that Ulrich’s conduct did not violate Section 631 because Ulrich was a party to the  
9 conversation and thus could not eavesdrop under the statute. *Id.* at 899. The Court wrote that “[i]t  
10 is never a secret to one party to a conversation that the other party is listening to the conversation;  
11 only a third party can listen secretly to a private conversation.” *Id.*

12 Thus, as the court observed in *Javier v. Assurance IQ, LLC*, the question for purposes of  
13 determining whether Salesforce was a party to the communications is whether Chat “is more akin  
14 to the tape recorder in *Rogers*, held by [Kaiser], or [to] the friend in *Ribas* (in which case, [Kaiser]  
15 is the wife who allowed [Salesforce] to listen in).” 2023 WL 114225, at \*5; *accord Yoon v.*  
16 *Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021). In analogous circumstances,  
17 courts have arrived at two different answers.

18 In the first set of cases, courts concluded that software providers are third parties. The  
19 Ninth Circuit in *In re Facebook, Inc. Internet Tracking Litigation* held that Facebook was not a  
20 party to communications between a user’s browser and a third-party website. 956 F.3d 589, 608  
21 (9th Cir. 2020). On websites with Facebook plug-ins, Facebook’s code copied a header containing  
22 a user’s personally identifiable URL information that was transmitted from the user’s web browser  
23 to the website. *Id.* at 607. This enabled Facebook to compile users’ browsing histories for its  
24 own purposes. *Id.* The Ninth Circuit concluded that “unknown duplication and communication  
25 of” information in this manner “do not exempt a defendant from liability under the party  
26 exception.” *Id.* at 608. Similarly, in *Revitch v. New Moosejaw, Inc.*, the court held that NaviStone  
27 was not a party to the communications between a website visitor and Moosejaw.com because  
28 Revitch had adequately alleged that NaviStone “embedded” code “into the Moosejaw.com pages”

that tracked interactions between users and the website. No. 18-cv-06827-VC, 2019 WL 5485330, at \*1 (N.D. Cal. Oct. 2023). The court emphasized that “it cannot be that anyone who receives a direct signal escapes liability by becoming a party to the communication,” *id.* at \*2, and further wrote,

Revitch began each communication by pressing a button on his mouse or a key on his keyboard, causing one signal to travel to his computer and then through his browser to Moosejaw’s server. Even if the browser caused a parallel signal to be sent to NaviStone, that intervention happened while the signal was already in transit from Revitch’s device. Section 631’s protections extend explicitly to the beginnings and ends of communications, so there is no reason to consider the first part of an electronic communication beyond the statute’s reach.

*Id.*

And in *Javier*, the court held that ActiveProspect was not a party to communications between Assurance IQ and users of its website. 2023 WL 114225, at \*5. ActiveProspect implemented “a piece of code that can be pasted into a form page to record keystrokes, mouse clicks, data entry, and other electronic communications of visitors to websites.” *Id.* at \*1 (internal quotation marks omitted). The website owner would subsequently obtain “a record of a users’ entire interaction with its website.” *Id.* Because Javier alleged “that ActiveProspect monitors, analyzes, and stores information about visits to assurance’s websites, and that ActiveProspect can use that information for other purposes,” ActiveProspect was not a party to the communication. *Id.* at \*6; *see also Yoon*, 549 F. Supp. 3d at 1081 (“Yoon’s first claim for relief survives Quantum Metric’s participant exception challenge because she alleges that QM captures, stores, and interprets her real-time data—which extends beyond the ordinary function of a tape recorder.”); *cf. Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 521 (C.D. Cal. 2021) (“FullStory did not become a ‘party’ to the communication simply because it was providing recording and transmission services for Nike.”).

In the second set of cases, courts have held that software providers are “extension[s]” that “provide[] a tool” allowing a company “to record and analyze its own data in aid of [its] business.” *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021). In *Graham*, FullStory provided a “software service that captures its clients’ data, hosts it on FullStory’s servers, and



allows the clients to analyze their data.” *Id.* The court likened this software to the tape recorder in *Rogers* and held that the software did not constitute eavesdropping because the plaintiffs had not alleged that FullStory “intercepted and used the data itself.” *Id.* In *Williams v. What If Holdings, LLC*, the court held that ActiveProspect’s software—the same software at issue in *Javier*—did not constitute wiretapping because there “were no facts . . . to suggest that ActiveProspect ‘intercepted and used the data itself.’” No. C 22-03780 WHA, 2023 WL 114225, at \*3 (N.D. Cal. Dec. 22, 2022) (quoting *Graham*, 533 F. Supp. 3d at 832); *see also Johnson v. Blue Nile, Inc.*, No. C 20-08183 LB, 2021 WL 1312771, at \*3 (N.D. Cal. Apr. 8, 2021); *Yale v. Clicktale, Inc.*, No. C 20-07575 LB, 2021 WL 1428400, at \*3 (N.D. Cal. Apr. 15, 2021).

The *Javier* court partially disagreed with the reading of Section 631 adopted by this second set of cases for two reasons. First, the reading “interprets the second prong of the statute . . . based on the intentions and usage of the prospective third party,” “[b]ut the third prong of the statute already penalizes ‘use.’” *Javier*, 2023 WL 114225, at \*6. As a result, “reading a use requirement into the second prong would add requirements that are not present (and swallow the third prong in the process).” *Id.*; *see Henson v. Santander Consumer USA Inc.*, 582 U.S. 79, 86 (2017) (“[W]hen we’re engaged in the business of interpreting statutes we presume differences in language . . . convey differences in meaning.”); *United States v. Jicarilla Apache Nation*, 564 U.S. 162, 185 (2011) (“[W]e are hesitant to adopt an interpretation of a congressional enactment which renders superfluous another portion of that same law.” (quoting *Mackey v. Lanier Collection Agency & Serv., Inc.*, 468 U.S. 825, 837 (1988))). Second, the California Supreme Court in *Ribas* did not consider the intention of the eavesdropper or the use of the obtained information, but rather “emphasized the privacy concerns at issue with having an ‘unannounced second auditor’ listening in on the call,” which implicates an individual’s “right to control the nature and extent of the firsthand dissemination of [their] statements.” *Id.*

The Court agrees with the *Javier* court that *Graham* and its progeny are based on a misinterpretation of Section 631 and *Ribas*, both of which compel the conclusion that the third party’s intentions with respect to the use of the collected information are irrelevant. Rather, the inquiry turns on the more granular question of whether the third party “ha[s] the *capability* to use



its record of the interaction for any other purpose.” *Javier*, 2023 WL 114225, at \*6 (emphasis altered). If Salesforce can use its records of the communications for any purpose other than to furnish information relating to those communications to Kaiser, then it is more like the wife in *Ribas* who allowed Clark to eavesdrop. By contrast, if Salesforce “has no independent ability to divulge its recording for any other purpose but for that of” Kaiser, then it is more like the tape recorder in *Rogers*. *Id.*

Plaintiffs allege that Chat “is run from Salesforce web servers,” ECF No. 22 ¶ 12, that communications over Chat are “routed through a Salesforce server,” *id.* ¶ 13, that Salesforce “directly receives the electronic communications of visitors,” *id.* ¶ 20, that Salesforce “analyzes the customer-support agent interactions in real time to create live transcripts of communications,” *id.* ¶ 14, and that “supervisors can view transcripts in real time,” *id.* ¶ 16. These allegations do not support a reasonable inference that Salesforce has the capability to use these communications for any purpose other than furnishing them to Kaiser. Chat, as alleged, is therefore more akin the tape recorder in *Rogers*, and Plaintiffs have thus failed to state a claim pursuant to Section 631.

## 2. Section 632

### a. Confidentiality of Communication

“Section 632 provides that ‘(a) every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records such confidential communication . . . shall be punished by fine . . . or by imprisonment.’” *Rattray v. City of National City*, 51 F.3d 793, 797 (9th Cir. 1994) (quoting Cal. Penal Code § 632). “A communication is confidential under Section 632 if a party ‘has an objectively reasonable expectation that the conversation is not being overheard or recorded.’” *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1073 (N.D. Cal. 2021) (quoting *Flanagan v. Flanagan*, 27 Cal. 4th 766, 776–77 (2002)). “California appeals courts have generally found that Internet-based communications are not ‘confidential’ within the meaning of [S]ection 632, because such communications can easily be shared by, for instance, the recipient(s) of the communications.” *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (collecting cases). As a result, courts “have developed a presumption” that such communications

1 do not give rise to the requisite expectation. *Revitch*, 2019 WL 5485330, at \*3.

2       Salesforce argues that Magpayo did not have a reasonable expectation of confidentiality  
3 because “chat communications are by their very nature non-confidential.” ECF No. 23 at 27  
4 (citing *Campbell*, 77 F. Supp. 3d at 849). Plaintiffs respond that Magpayo maintained a  
5 reasonable expectation of confidentiality because she communicated information related to her  
6 prescription history, medical conditions, and insurance information to the customer service agents  
7 in a healthcare context. ECF No. 28 at 23. The Court agrees with Plaintiffs that the context of  
8 these communications renders them confidential.

9       A recent case from this district is instructive. In *In re Meta Pixel Healthcare Litig.*, No.  
10 22-CV-03580-WHO, 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022), the plaintiffs alleged that a  
11 Meta software product called Pixel, when installed on the patient portal of the plaintiffs’  
12 healthcare providers, intercepted “data relating to patient portal logins and logouts alongside  
13 identifiers for each patient,” which was then transmitted to Meta. *Id.*, 2022 WL 17869218, at \*8.  
14 The plaintiffs further alleged that following login, “the Meta Pixel allegedly continue[d] to  
15 transmit information to Meta, including information about doctors, medical conditions, and  
16 appointments associated with a patient’s session.” *Id.*, 2022 WL 17869218, at \*3. Meta allegedly  
17 then “monetize[d] the information that it receive[d] through the Meta Pixel by using it to generate  
18 highly-profitable targeted advertising on-and off-Facebook.” *Id.* The plaintiffs brought several  
19 claims against Meta in connection with these practices, including claims under sections 631(a) and  
20 632(a). *Id.*, 2022 WL 17869218, at \*13.

21       As Salesforce does here, Meta argued that the plaintiffs had no reasonable expectation of  
22 privacy because the communications occurred over the internet, but the court rejected that  
23 argument:

24               Communications made in the context of a patient-medical provider  
25 relationship are readily distinguishable from online communications  
26 in general for at least two reasons. First, patient-status and medical-  
27 related communications between patients and their medical  
28 providers are protected by federal law . . . . Second, unlike  
communications made while inquiring about items of clothing on a  
retail website, *Revitch*, 2019 WL 5485330, at \*3, health-related  
communications with a medical provider are almost uniquely  
personal. “One can think of few subject areas more personal and

more likely to implicate privacy interests than that of one's health or genetic make-up." *Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1269 (9th Cir. 1998).

*Id.*, 2022 WL 17869218, at \*14–15 (additional citations omitted). The same is true of the communications at issue in the present case.

Salesforce does not meaningfully engage with this authority. Instead, it suggests that the operative complaint can be read so as to suggest that Plaintiffs were “merely using publicly-available customer support chats [and therefore] they had no objectively reasonable expectation that their communications were ‘confidential’ under the facts alleged.” ECF No. 31 at 18. Salesforce cites no authority for the proposition that communications with a health care provider must occur with only certain of its agents or employees to be confidential, or that such communications are not confidential if conducted with a customer support worker. The Court therefore rejects Salesforce’s argument and concludes that Magpayo’s communications were “confidential” within the meaning of Section 632.

#### **b. Consent**

Salesforce argues that Kaiser’s privacy policies “put [Magpayo] on prior notice, disclosing that [Kaiser] (i) collect[s] Plaintiffs’ PHI and (ii) use[s] service providers that aid in this collection and subsequent customer service functions,” such that Magpayo consented to Salesforce’s monitoring and recording. ECF No. 23 at 29. Plaintiffs respond that Magpayo accessed the chat function using a Kaiser web page that did not require Magpayo’s consent. ECF No. 28 at 31. Salesforce then replies that Plaintiffs make inconsistent allegations about which web pages Magpayo actually viewed, and that the only page that did not require a user’s consent before chatting “applies only to federal employees, which Magpayo does not allege she is or was.” ECF No. 31 at 20 (citing ECF No. 22 ¶ 19).

Salesforce’s arguments do not appear to be based on the operative complaint, which says nothing regarding whether the web page(s) Magpayo visited apply only to federal employees, or whether Magpayo is or was a federal employee. Nor need the Court resolve the parties’ disagreements about how to construe the allegations that Plaintiffs actually do make. Because there was at least one chat portal that did not require consent before use, and it is possible that

1 Magpayo used that portal, Salesforce has not established that Magpayo consented to the  
2 monitoring and recording of her communications. Salesforce’s motion to dismiss Plaintiffs’  
3 section 632 claim is therefore denied.

#### 4 C. WESCA

5 WESCA “operates in conjunction with and as a supplement to the Federal Wiretap Act, 18  
6 U.S.C. § 2150 *et seq.*” *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125–126 (3d Cir. 2022).  
7 The statute “offers a private civil cause of action to ‘[a]ny person whose wire, electronic or  
8 communication is intercepted, disclosed, or used’ . . . against ‘any person who intercepts,  
9 discloses, or procures any other person to intercept, disclose or use, such communication.” *Id.* at  
10 125 (quoting 18 Pa. Cons. Stat. § 5725(a)). WESCA defines “intercept” as “[a]ural or other  
11 acquisition of the contents of any wire, electronic or oral communication through the use of any  
12 electronic, mechanical, or other device.” 18 Pa. Const. Stat. § 5702. WESCA further defines  
13 “electronic, mechanical or other device” as “[a]ny apparatus . . . that can be used to intercept a  
14 wire, electronic or oral communication.” *Id.* That definition expressly excludes, in relevant part,  
15 “[a]ny telephone or telegraph instrument, equipment, or facility, or any component thereof  
16 furnished to the subscriber or user by a provider of wire or electronic communication service in  
17 the ordinary course of its business.” *Id.*

18 Salesforce first argues that Yockey has failed to allege that Salesforce intercepted his chat  
19 communications. The Third Circuit has written that “WESCA”s use of ‘intercept’ . . . reduces to  
20 acquiring certain communications using a device. And based on just that definition, anyone could  
21 ‘intercept’ communications, including people who ‘acquire’ a text message or chat sent to them.”  
22 *Popa*, 52 F.4th at 126. Thus, even if the communications at issue were sent directly through the  
23 Chat interface, Salesforce has nonetheless intercepted those communications within the meaning  
24 of WESCA to the extent that Salesforce received and stored those communications on its servers.

25 Salesforce next argues that WESCA exempts Chat from its definition of “electronic,  
26 mechanical or other device.” However, the definition exempts only instruments, equipment,  
27 facilities, or components appropriately characterized as “telephon[ic] or telegraph[ic].” 18 Pa.  
28 Const. Stat. § 5702. That a device “can perform functions similar or identical to a modern

telephone is” insufficient to bring that device within this “telephone exception.” *Commonwealth v. Diego*, 119 A.3d 370, 375 (Pa. Super. Ct. 2015). One court held, for example, that “telephone” in Section 5702 did not include an iPad because such an interpretation would “radically expand the definition of ‘telephone’ under [WESCA]” and run contrary to the requirement that WESCA’s provisions are to be “strictly construed.” *Id.* (quoting *Commonwealth v. Spangler*, 809 A.2d 234, 237 (Pa. 2002)). Therefore, Chat does not qualify as a “telephone or telegraph” even though it may be said to share features with such devices.

Third, Salesforce argues that Yockey’s allegations do not establish that his communications were rerouted contemporaneously with transmission. WESCA does not impose a rerouting requirement; rather, it requires that communications be intercepted. *See* 18 Pa. Cons. Stat. § 5725(a). Salesforce’s argument relies on a case in which the Third Circuit wrote, “Electronic communications are . . . ‘intercepted’ when software reroutes communications to an interceptor.” *Popa*, 52 F.4th at 130. The Third Circuit did not articulate such rerouting as a requirement of interception, but rather described the act of rerouting according to the facts of the case for purposes of determining where an interception occurs geographically. And while Salesforce is correct that an intercept must occur “contemporaneously with transmission” under WESCA, *see Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 & n.6 (3d Cir. 2003), Yockey plausibly alleges that Salesforce, in real time, directly receives Chat communications, creates live transcripts of those communications, and permits Rite Aid supervisors to view those transcripts. ECF No. 22 ¶¶ 13, 14, 16, 20. Yockey also plausibly alleges that Salesforce begins to obtain the contents of a user’s message before the user sends it via the Sneak Peek feature. *Id.* ¶ 23. Salesforce protests that the complaint is devoid of allegations that Salesforce personnel read or could read the messages before RiteAid, but Yockey alleges misconduct on the part of Salesforce as the provider, not on the part of its personnel.

Fourth, Salesforce argues that two of WESCA’s exceptions to liability apply to Salesforce’s conduct. The first exception provides that “[i]t shall not be unlawful . . . for:”

An officer, agent or employee of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that

communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of wire or electronic communication service. However, no provider of wire or electronic communication service shall utilize service observing or random monitoring except for mechanical or service quality control checks.

18 Pa. Const. Stat. § 5704(1). Salesforce argues that any interception is a “necessary incident to its rendition of [its] service.”

There are two problems with this argument. First, it is not clear that “provider” as that term is used in section 5704(1) refers to any entity other than Rite Aid, i.e., the only entity that is a “provider” of services to the Plaintiff. Thus, Salesforce has not established that it is entitled to invoke this protection. Next, the second sentence of the exception states that “no provider of wire or electronic communication service shall utilize service observing or random monitoring except for mechanical or service quality control checks.” 18 Pa. Const. Stat. § 5704(1). Whatever Salesforce is doing, it goes well beyond “service observing or random monitoring . . . for mechanical or service quality control checks.” See ECF No. 22 ¶¶ 21-23 (describing Salesforce’s “Sneak Peek” feature, which enables an agent to view the contents of a customer’s message while the customer types the message, *i.e.*, before the customer sends the message to the agent. *Id.* ¶ 22–23. For these reasons, the Court concludes that the exception set forth in section 5704(1) does not apply.

The second exception provides that “[i]t shall not be unlawful . . . for . . . [a] person or entity providing electronic communication service to the public to divulge the contents of any such communication . . . with the lawful consent of the originator or intended recipient of the communication.” 18 Pa. Const. Stat. § 5704(9). This provision “allows only one party [to] consent to the recording and disclosure involved in computer communications, electronic mail and voice mail.” *Barash v. Penn. Public Utility Comm’n*, 575 A.2d 79, 95 n.6 (1990) (Pellegrini, J., concurring in part and dissenting in part), *aff’d sub nom. Barash v. Bell Tel. Co. of Penn.*, 605 A.2d 1198 (Pa. 1992)). Salesforce does not directly provide Chat’s services to the public. Rather, Salesforce provides Chat to companies that contract with it to use the service on their websites. Even if those websites are accessible to Rite Aid’s customers, there is nonetheless a degree of



separation between Salesforce and the public that is absent typical from arrangements between service providers and members of the public, such as that of an e-mail service to an e-mail user. *Cf. Diego*, 119 A.3d at 376 (noting that “it is, at best, a dubious proposition that the authors of the 1978 [WESCA]” intended an exception to apply to technology “not invented until the late 1980’s”). And because the Pennsylvania Supreme Court has instructed that the WESCA’s provisions are to be “strictly construed,” the Court cannot conclude, as a matter of law, that the exception applies. *Spangler*, 809 A.2d at 23. Salesforce identifies no authority to the contrary, and the Court is aware of none. Therefore, Yockey has stated a WESCA claim.

#### **D. Consent**

Salesforce argues that Yockey otherwise consented to Salesforce’s conduct. *See* 18 Pa. Const. Stat. § 5704(1) (exempting from liability “[a] person . . . intercept[ing] a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interpretation”). Salesforce points to Rite Aid’s privacy policy, which appears via a hyperlink when using the “Chat With a Healthcare Professional” option. ECF No. 24-5 at 2.<sup>1</sup> The privacy policy discloses that Rite Aid “may share information about you with our service providers who perform services on our behalf. In addition, we may also share your personal information . . . with third parties who provide services that we offer through our Sites.” ECF no. 24-1 at 3. Yockey argues that he used the “Chat With Customer Support” option, which did not feature the hyperlink.

Regardless of whether the hyperlink to the privacy policy appeared in the particular chat window accessed by Yockey, the policy’s language does not encompass the conduct at issue. “[P]ersonal information” is not synonymous with a word-for-word transcript of all communications both as a matter of common sense and as defined by the policy. *See* ECF No. 24-

---

<sup>1</sup> Because Yockey alleges that he did not consent to the communications at issue, the Court considers the contents of the Rite Aid privacy policy under the incorporation by reference doctrine. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018). Salesforce’s requests for judicial notice, ECF Nos. 24 & 32, are otherwise denied because the Court need not rely on these materials to resolve the instant motion. The Court notes that judicial notice and incorporation by reference are separate procedures that “permit district courts to consider materials outside of a complaint . . . for different reasons and in different ways.” *Id.* at 998. It is therefore improper, as Salesforce does, to request the Court to take judicial notice of materials on the ground that those materials are incorporated by reference into the complaint.



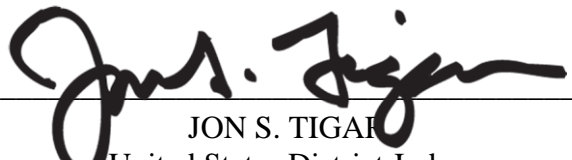
1 at 2; *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) (“In order for consent to be actual, the disclosures must ‘explicitly notify’ users of the practice at issue. (quoting *in re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at \*12 (N.D. Cal. Sept. 26, 2013))). And even if “personal information” encompassed a transcript of all communications, the policy does not disclose that Salesforce, via the Sneak Peek feature, obtains those communications while users type them.

### CONCLUSION

For the foregoing reasons, Salesforce’s motion is granted in part and denied in part. Dismissal of Magpayo’s CIPA Section 631 claim is with leave to amend because Salesforce has not shown that amendment would prejudice Salesforce, is sought in bad faith, would produce an undue delay, or would be futile. *See AmerisourceBergen Corp v. Dialyst West, Inc.*, 465 F.3d 946, 951 (9th Cir. 2006). Plaintiffs may file an amended complaint within twenty-one days of this order solely to cure the deficiencies identified by this order. Failure to file a timely amended complaint will result in dismissal of Magpayo’s CIPA Section 631 claim with prejudice.

**IT IS SO ORDERED.**

Dated: August 25, 2023

  
JON S. TIGAI  
United States District Judge